PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2000-092040**
(43)Date of publication of application : **31.03.2000**

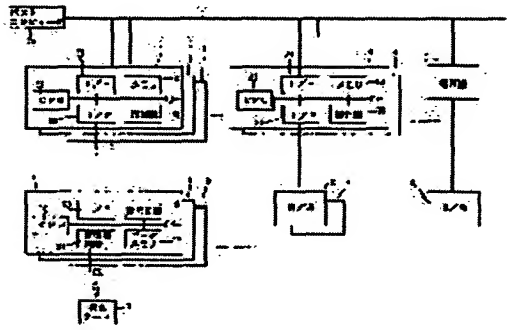
(51)Int.Cl. **H04L 9/10**
B42D 15/10
G06K 17/00
G07B 15/00
H04L 9/14
H04L 9/32

(21)Application number : **10-258016**
(22)Date of filing : **11.09.1998**

(71)Applicant : **OMRON CORP**
(72)Inventor : **WAKABAYASHI NAOYUKI**

(54) STORAGE MEDIUM, READER/WRITER, CARD SYSTEM, METHOD FOR USING CRYPTOGRAPHIC KEY, STATION SERVICE SYSTEM, AND CARD ISSUING MACHINE

(57)Abstract:
PROBLEM TO BE SOLVED: To update a cryptographic key as required, e.g. periodically or in case of possibility of a decoded cryptographic key without using all cryptographic keys at random by updating the cryptographic key selected by a command sent from a reader/writer.
SOLUTION: A reader/writer 6 stores old cryptographic keys that were used in the past and not in use at present and a cryptographic key that is currently in use. Furthermore, the reader/writer 6 transmits an update command to a passenger card 7 to allow the passenger card 7 to update its cryptographic key from an older cryptographic key to the cryptographic key used at present when the cryptographic key used by the passenger card 7 is the cryptographic key that was used in the past but not in use at present according to a response from the passenger card 7 as a result of communciation between the reader/writer 6 and the passenger card 7, and the passenger card 7 updates the cryptographic key into the cryptographic key used at present in response to the command. Thus, the cryptographic key of the old passenger card 7 having been issued before is finally updated into the cryptographic key used at present.



LEGAL STATUS

[Date of request for examination] 03.09.1999
[Date of sending the examiner's decision of rejection] 08.08.2000
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－92040
（P2000－92040A）
(43)公開日　平成12年３月31日(2000.3.31)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｈ０４Ｌ　9/10		Ｈ０４Ｌ　9/00	６２１Ａ	２Ｃ００５
Ｂ４２Ｄ　15/10	５２１	Ｂ４２Ｄ　15/10	５２１	５Ｂ０５８
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｓ	５Ｊ１０４
Ｇ０７Ｂ　15/00	５１０	Ｇ０７Ｂ　15/00	５１０	
Ｈ０４Ｌ　9/14		Ｈ０４Ｌ　9/00	６４１	

審査請求　有　請求項の数10　ＯＬ　（全 13 頁）　最終頁に続く

(21)出願番号　特願平10－258016

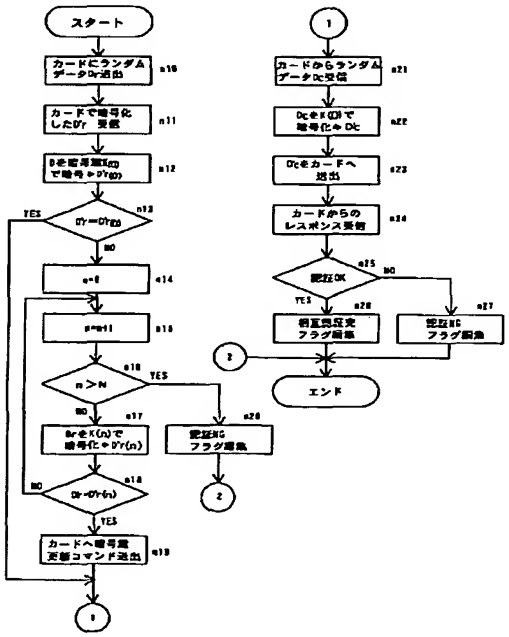
(22)出願日　平成10年９月11日(1998.9.11)

(71)出願人　000002945
オムロン株式会社
京都府京都市右京区花園土堂町10番地
(72)発明者　若林　尚之
京都府京都市右京区花園土堂町10番地　オムロン株式会社内
(74)代理人　100086737
弁理士　岡田　和秀

Ｆターム(参考)　2C005 MA03 MB07 NA09 SA02 SA03 SA05 SA06 SA07 TA21 TA22
5B058 KA11 KA33 KA35 YA20
5J104 AA16 EA02 EA18 NA02 NA33 PA11

(54)【発明の名称】　記憶媒体、読出／書込機、カードシステム、暗号鍵使用方法、駅務システムおよびカード発行機

(57)【要約】
【課題】　ＩＣカードなどの記憶媒体と読出／書込機との間の暗号処理などにおいて、使用する暗号鍵を、必要な時に更新できるとともに、複数の暗号鍵の全てが解読される危険性が低く、記憶媒体に記憶させている複数の暗号鍵を変更することができるようにする。
【解決手段】　ＩＣカードには、ＩＣカード発行時に、そのＩＣカード発行時点で使用している暗号鍵および今後使用する予定の暗号鍵の複数の暗号鍵を記憶させ、読出／書込機には、現在使用している暗号鍵と過去に使用した旧い複数の暗号鍵とを記憶させ、読出／書込機は、ＩＣカードからのリスポンスによって、ＩＣカードが使用している暗号鍵が、過去に使用した暗号鍵であるときには、現在使用している暗号鍵に更新するように更新コマンドを送出し、ＩＣカードは、そのコマンドに応答して使用する暗号鍵を更新するように構成している。



【特許請求の範囲】

【請求項１】　暗号鍵を用いて読出／書込機との間で認証および通信を行うよう構成された記憶媒体において、複数の暗号鍵を記憶する暗号鍵記憶手段と、前記暗号鍵記憶手段に記憶されている複数の暗号鍵のうちからいずれかを選択する暗号鍵選択手段と、前記読出／書込機から送出されるコマンドにより前記選択する暗号鍵を更新する暗号鍵更新手段とを具備したことを特徴とする記憶媒体。

【請求項２】　請求項１において、
前記暗号鍵記憶手段に記憶されている複数の暗号鍵の少なくとも一部の暗号鍵を読出／書込機から書き換えることを特徴とする記憶媒体。

【請求項３】　暗号鍵を用いて記憶媒体との間で認証および通信を行うよう構成された読出／書込機において、複数の暗号鍵を記憶する暗号鍵記憶手段と、前記暗号鍵記憶手段に記憶されている複数の暗号鍵のうちからいずれかを選択する暗号鍵選択手段と、前記記憶媒体からのレスポンスにより該記憶媒体が現在使用している暗号鍵が、当該読出／書込機で過去に使用された暗号鍵であるかどうかを知る暗号鍵知得手段と、前記記憶媒体が現在使用している暗号鍵が過去に使用された暗号鍵のときは、前記記憶媒体の暗号鍵を更新するコマンドを送出する暗号鍵更新コマンド送出手段とを具備したことを特徴とする読出／書込機。

【請求項４】　請求項３において、
上位機器からのコマンドにより、当該読出／書込機が使用する暗号鍵を変更する暗号鍵変更手段を具備したことを特徴とする読出／書込機。

【請求項５】　請求項３において、
前記記憶媒体が記憶している複数の暗号鍵の少なくとも一部の暗号鍵を書き換えることを特徴とする読出／書込機。

【請求項６】　請求項１または２に記載の記憶媒体をカードとし、該カードと、請求項３ないし５いずれかに記載の読出／書込機とを有し、カードが現在使用している暗号鍵が、前記読出／書込機で過去に使用された暗号鍵のときは、カードの暗号鍵を更新した後、その更新された暗号鍵を用いてカードと読出／書込機とが相互認証を行うことを特徴とするカードシステム。

【請求項７】　記憶媒体と読出／書込機それぞれには複数の暗号鍵を記憶させておき、
読出／書込機は、
記憶媒体から送信されてきた該記憶媒体が使用している暗号鍵による暗号化データと、読出／書込機が使用している暗号鍵により作成した暗号化データとを比較して記憶媒体および読出／書込機が使用している暗号鍵が一致しているか否かを判断し、一致していないときには、記憶媒体から送信されてきた前記暗号化データと、読出／書込機で過去に使用した暗号鍵により作成した暗号化データとを比較して記憶媒体が現在使用している暗号鍵が、過去に使用した暗号鍵であるか否かを判断し、前記過去に使用した暗号鍵であるときには、記憶媒体に対して、該記憶媒体が使用している暗号鍵を更新させる更新コマンドを送信し、
記憶媒体は、
前記更新コマンドに応答して、暗号鍵を更新することを特徴とする暗号鍵使用方法。

【請求項８】　請求項１または２に記載の記憶媒体を乗車カードとし、該乗車カードと、これに対する読み出し／書き込みを行う請求項３または４に記載の読出／書込機を備えた自動改札機とを有し、
読出／書込機は、
乗車カードから送信されてきた該乗車カードが使用している暗号鍵による暗号化データと、読出／書込機が使用している暗号鍵により作成した暗号化データとを比較して乗車カードおよび読出／書込機が使用している暗号鍵が一致しているか否かを判断し、一致していないときには、乗車カードから送信されてきた前記暗号化データと、読出／書込機で過去に使用した暗号鍵により作成した暗号化データとを比較して乗車カードが使用している暗号鍵が、過去に使用した暗号鍵であるか否かを判断し、過去に使用した暗号鍵であるときには、乗車カードに対して、該乗車カードが使用している暗号鍵を更新させる更新コマンドを送信し、
乗車カードは、
前記更新コマンドに応答して、暗号鍵を更新することを特徴とする駅務システム。

【請求項９】　請求項１または２に記載の記憶媒体を乗車カードとし、該乗車カードと、これに対する読み出し／書き込みを行う請求項５に記載の読出／書込機を備えたカード発行機とを有し、
読出／書込機は、乗車カードの発行時に、該乗車カードに記憶されている複数の暗号鍵を書き換えることを特徴とする駅務システム。

【請求項１０】　請求項１または２に記載の記憶媒体を乗車カードとし、該乗車カードの暗号鍵記憶手段に、現在使用する暗号鍵および将来使用する予定の複数の暗号鍵を書き込む一方、暗号鍵選択手段で前記現在使用する暗号鍵を選択するように設定して該乗車カードを発行するカード発行機。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、データを記憶する記憶媒体、この記憶媒体に対して読み出し／書き込みを行う読出／書込機、それらを用いたカードシステム、それらに好適な暗号鍵使用方法、および、それらを用いた自動改札などの駅務システム並びにカード発行機に関する。

【０００２】

【従来の技術】例えば、記憶媒体であるカードを自動料金徴収機の読出／書込機でカードの入出金などの処理をする場合、カードのセキュリティ性を確保する必要がある。そのため、通常、カードと読出／書込機との間で暗号を用いた相互認証や通信の暗号化が行われている。なお、相互認証とは、カード側からみて、通信相手となる読出／書込機が正当であるか、また読出／書込機側からみて、通信相手であるカードが正当であるかを、相互に認証することであるが、通常、相互に相手が正当な暗号鍵を知っているかどうかで判定する。

【０００３】

【発明が解決しようとする課題】上述の暗号処理においては、すべてのカードおよび読出／書込機も同じ暗号鍵（共通暗号鍵）を使用するようにした方式があるが、この方式では一旦、共通暗号鍵が他人に知られると、システム全体のセキュリティ性が損なわれてしまうという欠点がある。

【０００４】この欠点をなくすために、カードに複数の暗号鍵を記憶させ、また読出／書込機にもカードが有する複数の暗号鍵を記憶させておき、読出／書込機側ではカードとの間の暗号処理において、前記複数の暗号鍵のうちのいずれか１つの暗号鍵をランダムに用いることでセキュリティ性を高められるようにしたシステムがある。

【０００５】こうした場合に問題とされているのは、前記ランダムに暗号鍵を用いているうちに、複数の暗号鍵のすべてが傍受され解読されてしまう危険性があり、特に、カードと読出／書込機とが非接触で通信を行う場合に、その危険性が増大する。そこで、カードが記憶する複数の暗号鍵のすべてを他の複数の暗号鍵に一斉に変更させることが考えられるが、このような暗号鍵の変更は、多数のカードが発行されて使用されるというカードの利用形態から考えて実際上は不可能である。

【０００６】本発明は、上述の技術的課題に鑑みて為されたものであって、ランダムにすべての暗号鍵を使用するのではなく、必要な時、例えば、定期的あるいは暗号鍵が解読されたような虞れがある時に暗号鍵を更新できるようにし、しかも、記憶媒体の複数の暗号鍵の変更を一斉に行う必要がないようにすることを目的とする。

【０００７】

【課題を解決するための手段】本発明では、上述の目的を達成するために、次のように構成している。

【０００８】すなわち、請求項１の本発明の記憶媒体は、暗号鍵を用いて読出／書込機との間で認証および通信を行うよう構成された記憶媒体において、複数の暗号鍵を記憶する暗号鍵記憶手段と、前記暗号鍵記憶手段に記憶されている複数の暗号鍵のうちからいずれかを選択する暗号鍵選択手段と、前記読出／書込機から送出されるコマンドにより前記選択する暗号鍵を更新する暗号鍵更新手段とを具備している。

【０００９】ここで、更新とは、使用している暗号鍵を、複数の暗号鍵の内の別の暗号鍵に切り換えて使用することをいい、更新の度に、複数の暗号鍵の内の一つの暗号鍵が、それまで使用していた暗号鍵に代えて使用されることになる。

【００１０】また、記憶媒体と読出／書込機との間の通信は、有線方式または無線方式のいずれの方式であってもよい。

【００１１】請求項２の本発明の記憶媒体は、請求項１において、前記暗号鍵記憶手段に記憶されている複数の暗号鍵の少なくとも一部の暗号鍵を読出／書込機から書き換えるものである。

【００１２】請求項３の本発明の読出／書込機は、暗号鍵を用いて記憶媒体との間で認証および通信を行うよう構成された読出／書込機において、複数の暗号鍵を記憶する暗号鍵記憶手段と、前記暗号鍵記憶手段に記憶されている複数の暗号鍵のうちからいずれかを選択する暗号鍵選択手段と、前記記憶媒体からのレスポンスにより該記憶媒体が現在使用している暗号鍵が、当該読出／書込機で過去に使用された暗号鍵であるかどうかを知る暗号鍵知得手段と、前記記憶媒体が現在使用している暗号鍵が過去に使用された暗号鍵のときは、前記記憶媒体の暗号鍵を更新するコマンドを送出する暗号鍵更新コマンド送出手段とを具備している。

【００１３】請求項４の本発明の読出／書込機は、請求項３において、上位機器からのコマンドにより、当該読出／書込機が使用する暗号鍵を変更する暗号鍵変更手段を具備している。

【００１４】請求項５の本発明の読出／書込機は、請求項３において、前記記憶媒体が記憶している複数の暗号鍵の少なくとも一部の暗号鍵を書き換えるものである。

【００１５】請求項６の本発明のカードシステムは、請求項１または２に記載の記憶媒体をカードとし、該カードと、請求項３ないし５いずれかに記載の読出／書込機とを有し、カードが現在使用している暗号鍵が、読出／書込機で過去に使用された暗号鍵のときは、カードの暗号鍵を更新した後、その更新された暗号鍵を用いてカードと読出／書込機とが相互認証を行うものである。

【００１６】請求項７の本発明の暗号鍵使用方法は、記憶媒体と読出／書込機それぞれには複数の暗号鍵を記憶させておき、読出／書込機は、記憶媒体から送信されてきた該記憶媒体が使用している暗号鍵による暗号化データと、読出／書込機が使用している暗号鍵により作成した暗号化データとを比較して記憶媒体および読出／書込機が使用している暗号鍵が一致しているか否かを判断し、一致していないときには、記憶媒体から送信されてきた前記暗号化データと、読出／書込機で過去に使用した暗号鍵により作成した暗号化データとを比較して記憶媒体が使用している暗号鍵が、過去に使用した暗号鍵であるか否かを判断し、過去に使用した暗号鍵であるとき

には、記憶媒体に対して、該記憶媒体が使用している暗号鍵を更新させる更新コマンドを送信し、記憶媒体は、前記更新コマンドに応答して、暗号鍵を更新するものである。

【００１７】請求項８の本発明の駅務システムは、請求項１または２に記載の記憶媒体を乗車カードとし、該乗車カードと、これに対する読み出し／書き込みを行う請求項３または４に記載の読出／書込機を備えた自動改札機とを有し、読出／書込機は、乗車カードから送信されてきた該乗車カードが使用している暗号鍵による暗号化データと、読出／書込機が使用している暗号鍵により作成した暗号化データとを比較して乗車カードおよび読出／書込機が使用している暗号鍵が一致しているか否かを判断し、一致していないときには、乗車カードから送信されてきた前記暗号化データと、読出／書込機で過去に使用した暗号鍵により作成した暗号化データとを比較して乗車カードが使用している暗号鍵が、過去に使用した暗号鍵であるか否かを判断し、過去に使用した暗号鍵であるときには、乗車カードに対して、該乗車カードが使用している暗号鍵を更新させる更新コマンドを送信し、乗車カードは、前記更新コマンドに応答して、暗号鍵を更新するものである。

【００１８】請求項９の本発明の駅務システムは、請求項１または２に記載の記憶媒体を乗車カードとし、該乗車カードと、これに対する読み出し／書き込みを行う請求項５に記載の読出／書込機を備えたカード発行機とを有し、読出／書込機は、乗車カードの発行時に、該乗車カードに記憶されている複数の暗号鍵を書き換えるものである。

【００１９】請求項１０の本発明のカード発行機は、請求項１または２に記載の記憶媒体を乗車カードとし、該乗車カードの暗号鍵記憶手段に、現在使用する暗号鍵および将来使用する予定の複数の暗号鍵を書き込む一方、暗号鍵選択手段で前記現在使用する暗号鍵を選択するように設定して該乗車カードを発行するものである。

【００２０】（作用）請求項１の記憶媒体によれば、読出／書込機との間の暗号処理において、複数の暗号鍵のいずれかを用いて暗号処理を行うので、共通暗号鍵方式のように一つの共通暗号鍵が解読されてもシステム全体のセキュリティ性が損なわれることがなく、また、使用する暗号鍵も読出／書込機からのコマンドによって必要に応じて更新されるので、ランダムにすべての暗号鍵を用いる従来例のように、全ての暗号鍵が傍受されて解読される虞れが低い。

【００２１】請求項２の記憶媒体によれば、記憶されている複数の暗号鍵が更新によって全て使用されてしまうまでに、複数の暗号鍵の少なくとも一部の暗号鍵を読出／書込機から新たな暗号鍵に書き換えることができる。これによって、永続的に新しい暗号鍵への更新が可能となる。

【００２２】請求項３の読出／書込機によれば、記憶媒体が使用している暗号鍵が、読出／書込機で過去に使用された暗号鍵であるか否かを判断し、過去に使用されている暗号鍵であるときには、記憶媒体に更新コマンドを送出して記憶媒体が使用する暗号鍵を更新することができるので、記憶媒体の暗号鍵を、読出／書込機が現在使用している最新の暗号鍵に一致させることができる。

【００２３】請求項４の読出／書込機によれば、上位機器からのコマンドによって使用する暗号鍵が変更されるので、必要に応じて、例えば、定期的あるいは現在使用している暗号鍵が解読される虞れがあるような時に、上位機器からのコマンドによって使用する暗号鍵を、新しい暗号鍵に変更できることになり、さらに、請求項３の作用によって、記憶媒体が使用する暗号鍵もその変更された暗号鍵に一致させることができる。

【００２４】請求項５の読出／書込機によれば、記憶媒体が記憶している複数の暗号鍵の少なくとも一部の暗号鍵を書き換えるので、記憶媒体の暗号鍵が順次更新されて記憶されている全ての暗号鍵が使用されてしまうまでに、新たな暗号鍵に書き換えることができ、これによって、永続的に新しい暗号鍵への更新が可能となる。

【００２５】請求項６のカードシステムによれば、カードと読出／書込機との暗号鍵が一致しなくても、カードの暗号鍵が、過去に使用した暗号鍵であれば、カードの暗号鍵が更新されて読出／書込機の暗号鍵に一致するので、相互認証が可能となる。

【００２６】請求項７の暗号鍵使用方法によれば、読出／書込機は、記憶媒体からの暗号化データと作成した暗号化データとを比較することにより、記憶媒体の暗号鍵が、読出／書込機が使用している暗号鍵に一致しているか否かを判断し、一致していないときには、記憶媒体の暗号鍵が、読出／書込機で過去に使用した暗号鍵であるか否かを判断し、過去の暗号鍵であるときには、記憶媒体の暗号鍵を更新させるので、記憶媒体の暗号鍵と読出／書込機との暗号鍵を一致させることができる。

【００２７】請求項８の駅務システムによれば、乗車カードと自動改札機の読出／書込機との間の暗号処理において、乗車カードおよび読出／書込機は、複数の暗号鍵を記憶しているので、一つの共通暗号鍵のみを記憶している共通暗号鍵方式のように共通暗号鍵が解読されてもシステム全体のセキュリティ性が損なわれることがなく、また、使用する暗号鍵も読出／書込機からのコマンドによって必要に応じて更新されるので、ランダムにすべての暗号鍵を用いる従来例のように、すべての暗号鍵が傍受されて解読される虞れが低い。

【００２８】請求項９の駅務システムによれば、カード発行機は、乗車カードの発行時に、乗車カードに記憶されている複数の暗号鍵を書き換えるので、永続的に新しい暗号鍵への更新が可能となる。

【００２９】請求項１０のカード発行機によれば、それ

まで使用された乗車カードを回収して新たな乗車カードとして発行するのではなく、使用されたことのない全く新規な乗車カードの発行時において、相互認証などを行うことなく、現在使用する暗号鍵および将来使用する予定の複数の暗号鍵を書き込むとともに、現在使用する暗号鍵を選択するよう設定して乗車カードを発行できる。

【００３０】

【発明の実施の形態】以下、図面によって本発明の実施の形態について詳細に説明する。

【００３１】図１は、本発明が適用される駅務システムの全体構成を示す図であり、同図において、７は記憶媒体（例えば、非接触通信ＩＣカード）としての定期券などの乗車カード、６はこの乗車カード７との間で非接触通信を行う読出／書込機（リーダ／ライタ）、１は読出／書込機６を備えた自動改札機、４は読出／書込機６を備えたカード発行機、５は読出／書込機６を備えた精算機であり、２５はこれらを制御するホストコンピュータである。自動改札機１および精算機４は、駅の構内に、複数台設置されている。

【００３２】乗車カード７は、カード発行機４で発行される。この発行された乗車カード７には、乗車区間とか使用有効期限等のデータが記録される。利用者は、発行された乗車カードやを用いて自動改札機１の改札を受ける。カード発行機４も自動改札機１も読出／書込機６を備えている。カード発行機４および自動改札機１は、読出／書込機６に対する上位機器となる。また、ホストコンピュータ２５は、カード発行機４および自動改札機１などに対する上位機器となる。自動改札機１は、ＣＰＵ２６、ホストコンピュータ２５および読出／書込機６のと間のインタフェース回路２７，２８、メモリ２９および扉制御回路３０などを備えており、カード発行機４は、ＣＰＵ３１、ホストコンピュータ２５および読出／書込機６との間のインタフェース回路３２，３３、メモリ３４およびカード発行のための操作盤３５などを備えている。なお、読出／書込機６を構成するブロックには、後述の説明で使用する参照符号を付している。

【００３３】ここで、システムの主要な構成の説明に先立って、この実施の形態の暗号鍵の使用方法についての概要を説明する。

【００３４】乗車カード７と読出／書込機６との間では、セキュリティ性を確保するために、暗号鍵を用いた認証や通信を行うのであるが、この実施の形態では、従来例の暗号処理方式の欠点を解消するために、次のように構成している。

【００３５】すなわち、乗車カード７には、カード発行時に、今後使用する予定の複数の暗号鍵を記憶させておき、その複数の暗号鍵の内の予め定めた暗号鍵（例えば、カード発行時点において使用すべき暗号鍵）を使用するように設定しておき、読出／書込機６からの更新コマンドがあったときには、そのコマンドで指定された暗号鍵に更新してその更新された暗号鍵を使用するように構成している。

【００３６】乗車カード７は、多数が長い期間に亘って順次的に発行されるために、乗車カード７に記憶される複数の暗号鍵の内容も必要に応じて新しい暗号鍵に順次的に切り換えられ、したがって、当初に発行された乗車カード７に記憶されている複数の暗号鍵（例えば、Ｋ１，Ｋ２，Ｋ３，Ｋ４．Ｋ５）と、後に発行される乗車カード７に記憶される複数の暗号鍵（例えば、Ｋ２，Ｋ３，Ｋ４，Ｋ５，Ｋ６）とは、共通する暗号鍵（Ｋ２，Ｋ３，Ｋ４，Ｋ５）が存在するけれども、当初の乗車カード７には、後の乗車カード７に記憶されていない旧い暗号鍵（Ｋ１）が記憶されている一方、後の乗車カード７には、当初の乗車カード７に記憶されていない将来使用する予定の新規な暗号鍵（Ｋ６）が記憶される場合が生じることになる。

【００３７】そして、全ての乗車カード７に共通に記憶されている複数の暗号鍵が、使用可能な暗号鍵となり、その複数の暗号鍵が順番で使用されることになる。

【００３８】一方、読出／書込機６には、過去に使用されて現在は使用されていない旧い暗号鍵（例えば、Ｋ１）および現在使用されている暗号鍵（例えば、Ｋ２）が少なくとも記憶されており、この暗号鍵（例えばＫ２）を使用する。

【００３９】さらに、読出／書込機６では、乗車カード７との間の通信において、乗車カード７のレスポンスからその乗車カード７が使用している暗号鍵が、過去に使用されて現在使用されていない暗号鍵（例えばＫ１）であれば、乗車カード７に対して、現在使用されている暗号鍵（例えばＫ２）に更新するように更新コマンドを送出し、これに応答してその乗車カード７は、現在使用されている暗号鍵（例えばＫ２）に更新するのである。

【００４０】したがって、当初発行された旧い乗車カード７は、読出／書込機６との通信によって、最終的に現在使用されている暗号鍵（例えばＫ２）に更新されて統一されることになる。

【００４１】システムのセキュリティ性を確保するために、定期的に、あるいは、現在使用されている暗号鍵が解読された虞れがあるような時には、上位機器である自動改札機１などからの変更コマンドによって、読出／書込機６は、現在使用している暗号鍵（例えば、Ｋ２）を、次に使用すべ暗号鍵（例えば、Ｋ３）に変更する一方、それまで使用していた暗号鍵（Ｋ２）を、旧い暗号鍵として追加し、以後、この変更した暗号鍵（Ｋ３）を使用する。したがって、この時点では、読出／書込機６には、過去に使用して現在使用されていない複数の暗号鍵（例えば、Ｋ１，Ｋ２）および現在使用されている暗号鍵（例えば、Ｋ３）が記憶されることになる。

【００４２】上位機器からの変更コマンドによって暗号鍵を変更した読出／書込機６と乗車カード７との通信に

よって、乗車カード７が、現在使用されていない過去に使用されていた暗号鍵（例えば、Ｋ２）を使用していたときには、読出／書込機６は、その乗車カード７に対して、現在使用されている暗号鍵（例えばＫ３）に更新するように更新コマンドを送出し、これに応答してその乗車カード７は、現在使用されている暗号鍵（例えばＫ３）に更新するのである。

【００４３】したがって、乗車カード７は、読出／書込機６との通信によって、最終的に現在使用されている暗号鍵（例えばＫ３）に更新されて統一されることになる。

【００４４】このように複数の暗号鍵を必要に応じて順次更新して暗号処理を行うので、共通暗号鍵方式のように一つの共通暗号鍵が解読されてもシステム全体のセキュリティ性が損なわれることがなく、また、使用する暗号鍵も読出／書込機６からの更新コマンドによって必要に応じて更新されるので、ランダムに全ての暗号鍵を用いる従来例のように、全ての暗号鍵が傍受されて解読される虞れが低い。

【００４５】さらに、乗車カード７の暗号鍵の更新も、読出／書込機６との通信による更新コマンドによって行われるので、全ての乗車カード７の複数の暗号鍵を一斉に変更するといった必要がない。

【００４６】以下、この乗車カード７および読出／書込機６等の主要な構成について詳細に説明する。

【００４７】図２は、この実施の形態の読出／書込機を備えた自動改札機１の外観斜視図であり、この自動改札機１は、改札通路３６を隔てて相対向する一対の改札機本体２を備える。両改札機本体２の側面それぞれには、改札通路３６の通過を許可あるいは阻止する図示しない扉が配備されている。各改札機本体２には、読出／書込機６が設けられており、そのアンテナコイル２３が各改札機本体２の上面に臨むように配設されている。

【００４８】このアンテナコイル２３は、定期券等の乗車カード７が備えるアンテナコイルが通信エリア内に位置したときに、その乗車カード７のアンテナコイルとの間で非接触でデータ通信が可能となっている。乗車カード７を携帯する利用者は、図２に示すように、その乗車カード７を改札機本体２に設けられた読出／書込機６のアンテナコイル２３との通信のための通信エリアにかざすだけでデータ通信が可能となる。

【００４９】読出／書込機６は乗車カード７と通信を行い、上位機器である自動改札機１は、その通信に基づいて乗車カード７の真偽および乗車条件などを判定し、これに基づいて、扉を制御して開放したり、閉止したりする。

【００５０】本実施の形態の乗車カード７は、上述のように複数の暗号鍵を記憶しており、それら複数の暗号鍵の中からある１つの暗号鍵を用いて暗号化とか復号化を行い、また、自動改札機１の読出／書込機６の更新コマンドにより現在使用している暗号鍵を次に使用する暗号鍵に更新し、またカード発行機４などの読出／書込機によって、カード発行時に、記憶している複数の全ての暗号鍵が書き換えられるようにしている。なお、カード発行時には、乗車カード７の複数の暗号鍵の全てではなく、使用済みの暗号鍵のみを新たな暗号鍵に書き換えるようにしてもよい。

【００５１】以下、図３を参照して、乗車カード７について説明する。乗車カード７は、内部にＣＰＵ８、プログラムメモリ９、データメモリ１０、暗号鍵記憶メモリ１１、暗号回路１２および変復調電源回路１３ならびにアンテナコイル１４を有している。

【００５２】ＣＰＵ８は、プログラムメモリ９に格納されているプログラムデータと、データメモリ１０に格納されているワーキングデータとを用いて、アンテナコイル１４を通じて受信した読出／書込機６からのコマンドに基づく処理を行うとともに、読出／書込機６に対してデータ送信の処理を行う。

【００５３】カード読出／書込機６から乗車カード７に送出されてくるコマンドには、ポーリング、認証、データの読み出しと書き込み、禁止などがある。ＣＰＵ８は、カード読出／書込機６からのこうした送出コマンドをアンテナコイル１４で受信し、変復調回路１３で復調し、暗号回路１２で復号する等の処理を行わせた後に取り込んで解析するとともに、この解析したコマンドに従った処理を実行するようになっている。

【００５４】暗号鍵記憶メモリ１１には、暗号鍵記憶手段として、図４で示すように乗車カード７の発行時に、カード発行機４の読出／書込機６によって、乗車カード７が自動改札機１の読出／書込機６などとの間で今後使用する予定である複数の暗号鍵（暗号鍵１，暗号鍵２，暗号鍵３，…，暗号鍵ｎ）が記憶させられている。暗号鍵記憶メモリ１１からは、これら複数の暗号鍵の読み出しは外部から一切できないハードウェア構成とされて不正に外部から暗号鍵が読み出せないようになっている。このハードウェア構成は、暗号鍵記憶メモリ１１をＣＰＵ８と同じＬＳＩチップに設け、このＬＳＩチップにテストピンを当てて信号を与えても暗号鍵は出力されず、あるいは、テスト端子をなくし、暗号鍵記憶メモリ１１からのデータの読み出しは、ＬＳＩチップ内のＣＰＵ８のみができるようにし、ＣＰＵ８と暗号鍵記憶メモリ１１間のバスは、ＬＳＩチップの外には、端子として出さないようにすればよい。これによって、ＬＳＩチップの外部（回路の外）から暗号鍵の読み出しを一切できないようにすることができる。

【００５５】ＣＰＵ８は、暗号鍵選択手段として、暗号鍵記憶メモリ１１に記憶されている図４の暗号鍵１，暗号鍵２，暗号鍵３，…，暗号鍵ｎから予め設定されている１つの暗号鍵を選択し、これを暗号回路１２に入力するようになっている。通常、カード発行時には、その時

点で使用されている暗号鍵１と、今後順番に使用されていく予定の複数の暗号鍵２，３，…が記憶させられるので、当初は、暗号鍵１を使用すべき暗号鍵として設定されている。

【００５６】その後、自動改札機１の読出／書込機６から更新コマンドがあれば、ＣＰＵ８は、暗号鍵更新手段として、そのコマンドに従って現在設定されている暗号鍵から更新コマンドで指定された他の暗号鍵に設定を更新したうえで、これを暗号回路１２に入力するようになっている。

【００５７】暗号回路１２は、上述のようにして選択された暗号鍵を用いて暗号化、復号化を行うものであり、自動改札機１の読出／書込機６との相互認証においても使用される。勿論、本実施の形態における乗車カード７は読出／書込機６との間での相互認証の後でのみデータの読み出しや書き込みのコマンドを受け付けるようになっている。

【００５８】変復調電源回路１３は、自動改札機１の読出／書込機６へ送信するデータの変調、読出／書込機６から受信したデータの復調、アンテナコイル１４で受けた読出／書込機６からの送信磁界により乗車カード７の電源を生成するようになっている。

【００５９】本実施の形態の読出／書込機６は、暗号鍵を用いて乗車カード７との間で認証および通信を行うよう構成されたものであって、複数の暗号鍵を記憶する暗号鍵記憶手段と、前記暗号鍵記憶手段に記憶されている複数の暗号鍵のうちからいずれかを選択する暗号鍵選択手段と、前記乗車カードからのレスポンスにより乗車カードで現在使用されている暗号鍵が、過去に使用されたいずれの暗号鍵であるかを知る暗号鍵知得手段と、乗車カードで現在使用されている暗号鍵が過去に使用されていた暗号鍵のときは、乗車カードの暗号鍵を更新するコマンドを送出するコマンド送出手段と、上位機器からのコマンドにより、当該読出／書込機が使用する暗号鍵を変更する暗号鍵変更手段とを具備している。

【００６０】以下、図５を参照して読出／書込機６について説明する。この読出／書込機６は、ＣＰＵ１５、プログラムメモリ１６、データメモリ１７、暗号回路１８、乗車カード用暗号鍵記憶メモリ１９、上位機器用暗号鍵記憶メモリ２０、上位機器用インタフェース２１および変復調回路２２ならびにアンテナコイル２３を有している。上位機器とは、上述のように、自動改札機１あるいはカード発行機４などである。

【００６１】自動改札機１は、読出／書込機６の他に扉の駆動機構を制御したり、ホストコンピュータ２５と通信を行うものであり、読出／書込機６の上位機器用インタフェース２１を介して接続されている。

【００６２】読出／書込機６は、電源投入時に、上位機器である自動改札機１などとの間でも相互認証を行い、接続のセキュリティ性を確保し、それ以降の自動改札機などの上位機器におけるアプリケーションに応じた処理を行うようになっている。

【００６３】システムのセキュリティ性を確保するために、現在使用されている暗号鍵の使用期間が一定期間に達したり、あるいは、現在使用されている暗号鍵が解読された虞れがあるような場合には、例えば、ホストコンピュータ２５から上位機器である自動改札機１などを介して読出／書込機６のＣＰＵ１５に対して、現在使用している暗号鍵を変更するコマンドが与えられ、これによって、乗車カード用暗号鍵記憶メモリ１９の暗号鍵が後述のように書き換えられて変更される。その後、読出／書込機６は、変更した暗号鍵で乗車カード７との処理を行うようになっている。

【００６４】図６は、暗号鍵の使用期間の一例を示す図であり、この例は、暗号鍵の解読といった事態が生じることなく順調に経過すれば、三カ月毎に暗号鍵を変更するものであり、暗号鍵１は、１９９８年１月１日から同年３月３１日までの三カ月間既に使用され、その後、暗号鍵２が現在使用中であり、順調に経過すれば、１９９８年６月３０日まで暗号鍵２が使用される予定であり、１９９８年７月１日からは暗号鍵３に変更されて暗号鍵３が使用される予定である。

【００６５】次に、読出／書込機６の動作について説明する。読出／書込機６は、上位機器用インタフェース２１を通して自動改札機１などの上位機器から受信したコマンドを復号し、復号したコマンドをＣＰＵ１５で解析し、そのコマンドに従った処理を実行する。上位機器からのコマンドが、例えば乗車カード７のデータメモリ１０に記憶されている乗車カード７に関するデータ、例えば定期券の有効期間、定期券の乗車区間というデータを読み出すというコマンドであれば、乗車カード７のデータメモリ１０からデータを読み取るリードコマンドを、乗車カード用暗号鍵記憶メモリ１９から選択した暗号鍵を用いて暗号回路１８で暗号化させ、変復調回路２２で変調させたうえでアンテナコイル２３から乗車カード７に送信する。そして、乗車カード７から前記リードコマンドに対して返送されるレスポンスを受信すると、それを変復調回路２２で復調し、暗号回路１８で復号したうえで乗車カード７のデータを得る。そして、そのデータを、暗号回路１８で暗号化してレスポンスとして上位機器用インタフェース２１から上位機器に送信する。そして、上位機器、例えば自動改札機１は、このレスポンスから乗車カード７が正当であれば開閉ドアを開け、正当でなければ開閉ドアを開けないように制御する。

【００６６】ここで、読出／書込機６から乗車カード７に与えられるコマンドにはポーリング、認証、データの読み出しと書き込みなどの従来からのコマンドの他に、乗車カード７の暗号鍵更新コマンド、乗車カード７の暗号鍵書き換えコマンドがある。また、上位機器である自動改札装置やカード発行機などからのコマンドには、乗

車カード７との通信コマンド、認証、カード読出／書込機６に対するデータの読み出しと書き込みなどの従来からのコマンドの他に、乗車カード７の暗号鍵更新コマンド、乗車カード７の暗号鍵書き換えコマンド、カード読出／書込機６の暗号鍵書き換えコマンドがある。

【００６７】乗車カード用暗号鍵記憶メモリ１９は、図７で示すように乗車カード７との間で過去に使用していた暗号鍵（旧暗号鍵－m，…，旧暗号鍵－１）と現在使用している暗号鍵（現在の暗号鍵０）とが記憶されている。乗車カード用暗号鍵記憶メモリ１９は、書き込み専用であり、外部から読み出しできないハードウェア構成となっていて外部からの不正な暗号鍵の読み出しができないようになっている。このハードウェア構成については前述したのでその説明は省略する。この乗車カード用暗号鍵記憶メモリ１９に記憶されている複数の暗号鍵のうち、現在使用されている暗号鍵を用いて乗車カード７処理のための暗号化、復号が行われる。

【００６８】また、上位機器である自動改札機１などから現在使用している暗号鍵を変更すべきコマンドが与えられると、その変更コマンドに応じて、図７の現暗号鍵０が、変更すべき暗号鍵に書き換えられ、それまで使用されていた現暗号鍵０が、旧暗号鍵－１となり、それまでの旧暗号鍵－１が、旧暗号鍵－２となり、以下、順送りされた内容に書き換えられ、以後は、この書き換えられた現暗号鍵０を使用して処理が行われる。なお、最も旧い暗号鍵は、発行されているすべての乗車カード７で使用される虞れがなくなった時点で不要となるので、上書きして消去すればよい。

【００６９】また、この実施の形態では、読出／書込機６が使用する暗号鍵は、上位機器からの変更コマンドによって書き換えられるようにしたけれども、本発明の他の実施の形態として、読出／書込機６においても、今後使用する複数の暗号鍵を予め記憶させておき、上位機器からの更新コマンドによって現在使用する暗号鍵を変更するように構成してもよい。

【００７０】暗号回路１８は、暗号鍵を用いて平文の暗号化、暗号文の復号を行い、また、上位機器とか乗車カード７との通信文（コマンド、レスポンス）の暗号化、復号の他、上位機器と乗車カード７との相互認証においても使用される。乗車カード７は、通常、読出／書込機６との相互認証の終了後にその他のコマンドを受け付けるようになっている。

【００７１】次に、自動改札機１における処理を図８で示されるフローチャートを参照して説明する。

【００７２】乗車カード７が、改札機本体２の読出／書込機６と通信し得る通信エリア内に無いときは、読出／書込機６は常に１０ミリ秒程度の一定周期でポーリングコマンドをアンテナコイル２３から送出している（ステップｎ１）。前記通信エリアに乗車カード７が進入し、その乗車カード７からポーリングコマンドに対するレスポンスが返送されると（ステップｎ２）、読出／書込機６と乗車カード７との間の相互認証を行う（ステップｎ３）。この相互認証については図９を用いて後で説明する。相互認証がＯＫであれば、乗車カード７のデータの読み出しと乗車カード７へのデータの書き込みの処理を行い（ステップｎ４）、最後に読出／書込機６が次の乗車カード７に対するポーリングに対して、処理済みの乗車カード７が応答しないように応答禁止の処理をする（ステップｎ５）。

【００７３】次に図９を参照して前記相互認証について説明する。

【００７４】読出／書込機６から乗車カード７に対しランダムデータＤｒを送出する（ステップｎ１０）。乗車カード７は、該乗車カード７で使用している暗号鍵を用いてそのランダムデータＤを暗号化して暗号化データＤｒ’とし、その暗号化したデータＤｒ’を読出／書込機６に送信する。読出／書込機６は、そのデータＤｒ’を受信する一方（ステップｎ１１）、そのランダムデータＤｒを現在使用している暗号鍵Ｋ（０）を用いて暗号化して暗号化データＤｒ’（０）を得る（ステップｎ１２）。そして、読出／書込機６はその暗号化したデータＤｒ’（０）を乗車カード７から送信されてきた暗号化データＤｒ’と比較し（ステップｎ１３）、両データＤｒ’（０）とＤｒ’とが一致していれば乗車カード７が正しい乗車カード７と認証するが、一致しないときは乗車カード７が不正な乗車カード７であるか、それとも乗車カード７が使用している暗号鍵が旧い暗号鍵であるかのいずれかとなる。

【００７５】乗車カード７が正しい乗車カードと認証した場合、今度は、乗車カード７からランダムデータＤｃを受信し（ステップｎ２１）、このランダムデータＤｃを現在使用している暗号鍵Ｋ（０）で暗号化し（ステップｎ２２）、暗号化データＤｃ’として、乗車カード７に送出する（ステップｎ２３）。乗車カード７からこの送出に対するレスポンスを受信すると（ステップｎ２４）、受信内容から認証ＯＫの場合は（ステップｎ２５）、相互認証が完了し（ステップｎ２６）、ＯＫでない場合は相互認証ＮＧとする（ステップｎ２７）。

【００７６】ステップｎ１３において、乗車カード７が正しい乗車カードと認証しない場合は、読出／書込機６は、暗号鍵の番号を０に初期化（ｎ＝０）した上で（ステップｎ１４）、暗号鍵の番号を過去に使用していた旧い暗号鍵の番号にし（ｎ＝ｎ＋１）（ステップｎ１５）、この番号の暗号鍵Ｋ（ｎ）を用いてデータを暗号化し（ステップｎ１７）、乗車カード７から返送されてきた暗号文と一致するかを判断する（ステップｎ１８）。一致と判断できるまで、カード読出／書込機６が記憶している旧い暗号鍵を順次選択していき（ステップｎ１６）、番号がｎの旧い暗号鍵でＤｒ’＝Ｄｒ’（ｎ）となって一致した場合ではカード読出／書込機６

は、乗車カード７が使用していた暗号鍵はその番号の旧い暗号鍵Ｋ（ｎ）と判断し、乗車カード７に対して、現在使用されている暗号鍵Ｋ（０）に更新するように、すなわち、暗号鍵記憶メモリ１１のポインタｎの暗号鍵を使用している乗車カード７に対して、ポインタ０の暗号鍵に更新するように暗号鍵更新コマンドを送出し（ステップｎ１９）、乗車カード７が使用する暗号鍵をＫ（０）に更新させてステップｎ２１以降の処理を行って乗車カード７が正当なものであると認証する。

【００７７】また、乗車カード７の暗号鍵の更新後、新しい暗号鍵を用いて再度認証を行うようにしても構わない。なお、読出／書込機６が保有する旧い暗号鍵のいずれの暗号鍵でも暗号文が一致しなかったときには、その乗車カード７は不正な乗車カード７と判断する（ステップｎ２０）。

【００７８】次に、カード発行機４の読出／書込機６による処理について説明する。

【００７９】カード発行機４では、図１０で示されているようにポーリング、レスポンス受信、相互認証ＯＫについて図８と同様である。図１０で相互認証が終了すると、暗号鍵書き換えコマンドを送信し、乗車カード７の暗号鍵を含むデータの書き換えの処理を行う（ステップｎ４）。その際、乗車カード７の暗号鍵記憶メモリ１１の複数の暗号鍵を、現在使用する暗号鍵と今後使用する予定の複数の暗号鍵に書き換える（ステップｎ５）。これによって、乗車カード７は、当初は、現在使用する暗号鍵を選択して使用し、以後は、更新コマンドによって使用する暗号鍵を順番に更新する。

【００８０】なお、乗車カードが、使用されたカードを回収して発行するのではなく、全く、新規に乗車カードを発行する場合には、相互認証を行うことなく、現在使用する暗号鍵と今後使用する予定の複数の暗号鍵を書き込めばよい。

【００８１】上述の実施の形態では、自動改札などの駅務システムに適用したけれども、本発明は、かかるシステムに限定されるものではなく、自動料金徴収システムあるいはその他のシステムにも適用されるものである。

【００８２】また、上述の実施の形態では、非接触方式の通信に適用したけれども、本発明は、接触方式の通信にも適用され得る。

【００８３】

【発明の効果】以上のように本発明によれば次の効果を得られる。

【００８４】請求項１の本発明の記憶媒体によれば、読出／書込機との間の暗号処理において、複数の暗号鍵のいずれかを用いて暗号処理を行うので、共通暗号鍵方式のように一つの共通暗号鍵が解読されてもシステム全体のセキュリティ性が損なわれることがなく、また、使用する暗号鍵も読出／書込機からのコマンドによって必要に応じて更新されるので、ランダムにすべての暗号鍵を用いる従来例のように、すべての暗号鍵が傍受されて解読される虞れが低く、セキュリティ性が向上する。

【００８５】請求項２の本発明の記憶媒体によれば、複数の暗号鍵の少なくとも一部の暗号鍵を読出／書込機から書き換えることができるので、記憶されている複数の暗号鍵が更新によってすべて使用されてしまうまでに、新たな暗号鍵に書き換えることができ、これによって、永続的に新しい暗号鍵への更新が可能となり、セキュリティ性を永続的に確保できる。

【００８６】請求項３の本発明の読出／書込機によれば、記憶媒体が使用している暗号鍵が、過去に使用された暗号鍵であるか否かを判断し、読出／書込機で過去に使用されている暗号鍵であるときには、記憶媒体に更新コマンドを送出して記憶媒体が使用する暗号鍵を更新することができるので、記憶媒体の暗号鍵を、読出／書込機が現在使用している最新の暗号鍵に一致させることができる。したがって、記憶媒体が使用する暗号鍵を変更するために、記憶媒体を回収して暗号鍵を一斉に変更するといった困難な作業を行う必要がなく、記憶媒体が使用されて読出／書込機との間で通信を行うことにより、自動的に暗号鍵が変更されることになる。

【００８７】請求項４の本発明の読出／書込機によれば、上位機器からのコマンドによって使用する暗号鍵が変更されるので、必要に応じて、例えば、定期的あるいは現在使用している暗号鍵が解読される虞れがあるような時に、上位機器からのコマンドによって使用する暗号鍵を新しい暗号鍵に変更できることになり、セキュリティ性を確保でき、さらに、請求項３の作用によって、記憶媒体が使用する暗号鍵もその変更された暗号鍵に一致させることができる。

【００８８】請求項５の本発明の読出／書込機によれば、記憶媒体が記憶している複数の暗号鍵の少なくとも一部の暗号鍵を書き換えるので、記憶媒体の暗号鍵が順次更新されて記憶されている全ての暗号鍵が使用されてしまうまでに、新たな複数の暗号鍵に書き換えることができ、これによって、永続的に新しい暗号鍵への更新が可能となり、セキュリティ性を永続的に確保できる。

【００８９】請求項６の本発明のカードシステムによれば、カードと読出／書込機との暗号鍵が一致しなくても、カードの暗号鍵が、読出／書込機で過去に使用した暗号鍵であれば、カードの暗号鍵が更新されて読出／書込機の暗号鍵に一致するので、相互認証が可能となる。しかも、記憶媒体をカードとしているので、自動料金収集システムなどの各種の用途に好適に実施できることになり、請求項１ないし５の作用効果を顕著に奏することができる。

【００９０】請求項７の本発明の暗号鍵使用方法によれば、読出／書込機は、記憶媒体からの暗号化データと作成した暗号化データとを比較することにより、記憶媒体の暗号鍵が、読出／書込機が使用している暗号鍵に一致

しているか否かを判断し、一致していないときには、記憶媒体の暗号鍵が、過去に使用した暗号鍵であるか否かを判断し、過去の暗号鍵であるときには、記憶媒体の暗号鍵を更新させるので、記憶媒体の暗号鍵と読出／書込機との暗号鍵を一致させることができる。

【００９１】また、記憶媒体および読出／書込機は、複数の暗号鍵を記憶しているので、一つの共通暗号鍵のみを記憶している共通暗号鍵方式のように共通暗号鍵が解読されてもシステム全体のセキュリティ性が損なわれることがなく、また、使用する暗号鍵も読出／書込機からのコマンドによって必要に応じて更新されるので、ランダムにすべての暗号鍵を用いる従来例のように、すべての暗号鍵が傍受されて解読される虞れが低く、さらに、記憶媒体に記憶されている複数の暗号鍵を一斉に変更するといった必要もない。

【００９２】請求項８の本発明の駅務システムによれば、乗車カードと自動改札機の読出／書込機との間の暗号処理において、乗車カードおよび読出／書込機は、複数の暗号鍵を記憶しているので、一つの共通暗号鍵のみを記憶している共通暗号鍵方式のように共通暗号鍵が解読されてもシステム全体のセキュリティ性が損なわれることがなく、また、使用する暗号鍵も読出／書込機からのコマンドによって必要に応じて更新されるので、ランダムにすべての暗号鍵を用いる従来例のように、すべての暗号鍵が傍受されて解読される虞れが低く、さらに、乗車カードに記憶されている複数の暗号鍵を一斉に変更するといった必要もない。

【００９３】請求項９の本発明の駅務システムによれば、カード発行機は、乗車カードの発行時に、乗車カードに記憶されている複数の暗号鍵を書き換えるので、永続的に新しい暗号鍵への更新が可能となり、システムのセキュリティ性を永続的に確保できる。

【００９４】請求項１０の本発明のカード発行機によれば、回収した乗車カードを用いるのではなく、全く新規な乗車カードの発行時において、相互認証などを行うことなく、現在使用する暗号鍵および将来使用する予定の複数の暗号鍵を書き込むとともに、現在使用する暗号鍵を選択するよう設定して乗車カードを発行できる。

【図面の簡単な説明】

【図１】　本発明の実施形態に係るシステムの概略構成図である。

【図２】　自動改札機の斜視図である。

【図３】　乗車カードのブロック図である。

【図４】　乗車カードの暗号鍵記憶メモリの記憶内容を示す図である。

【図５】　読出／書込機のブロック図である。

【図６】　暗号鍵の使用期間を示す図である。

【図７】　読出／書込機の乗車カード用暗号鍵記憶メモリの記憶内容を示す図である。

【図８】　自動改札機の読出／書込機の動作説明に供するフローチャートである。

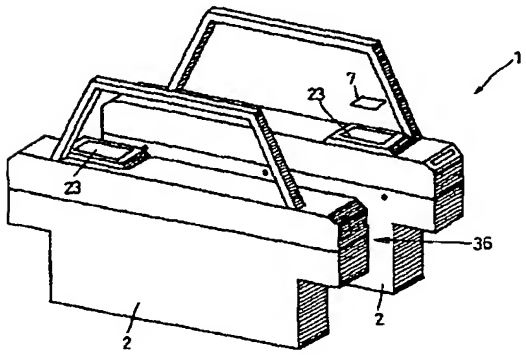
【図９】　相互認証の動作説明に供するフローチャートである。

【図１０】　カード発行機の読出／書込機の動作説明に供するフローチャートである。

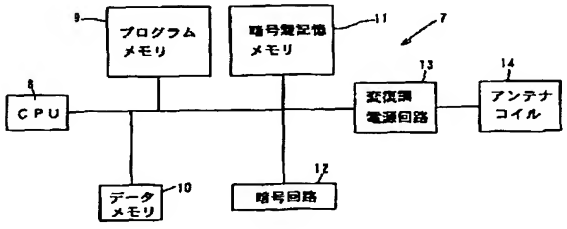
【符号の説明】

１	自動改札機
６	読出／書込機
７	乗車カード
８，１５	ＣＰＵ
１１	暗号鍵記憶メモリ
１４，２３	アンテナコイル
１９	乗車カード用暗号鍵記憶メモリ

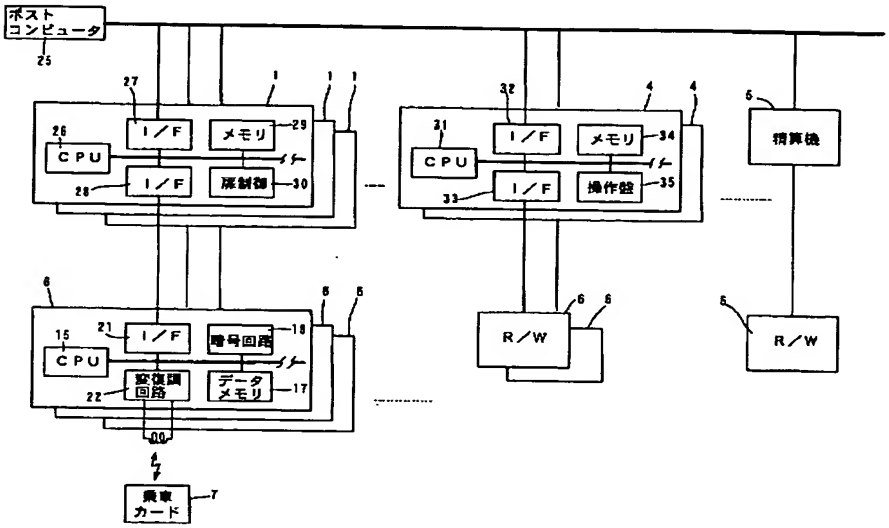
【図２】



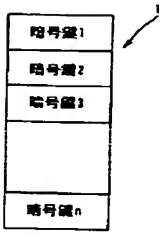
【図３】



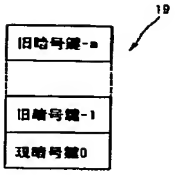
【図１】



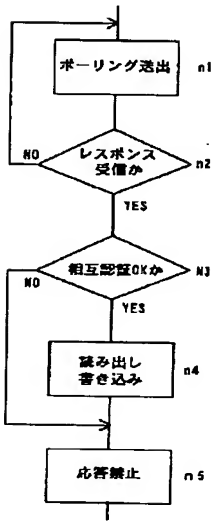
【図４】



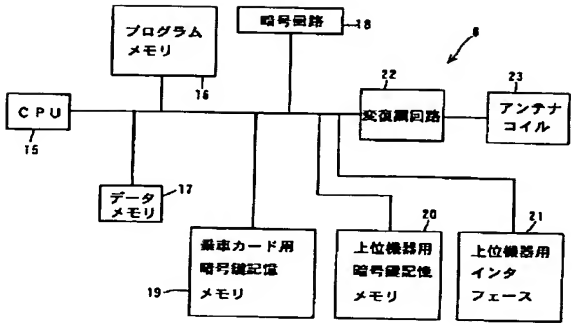
【図７】



【図８】



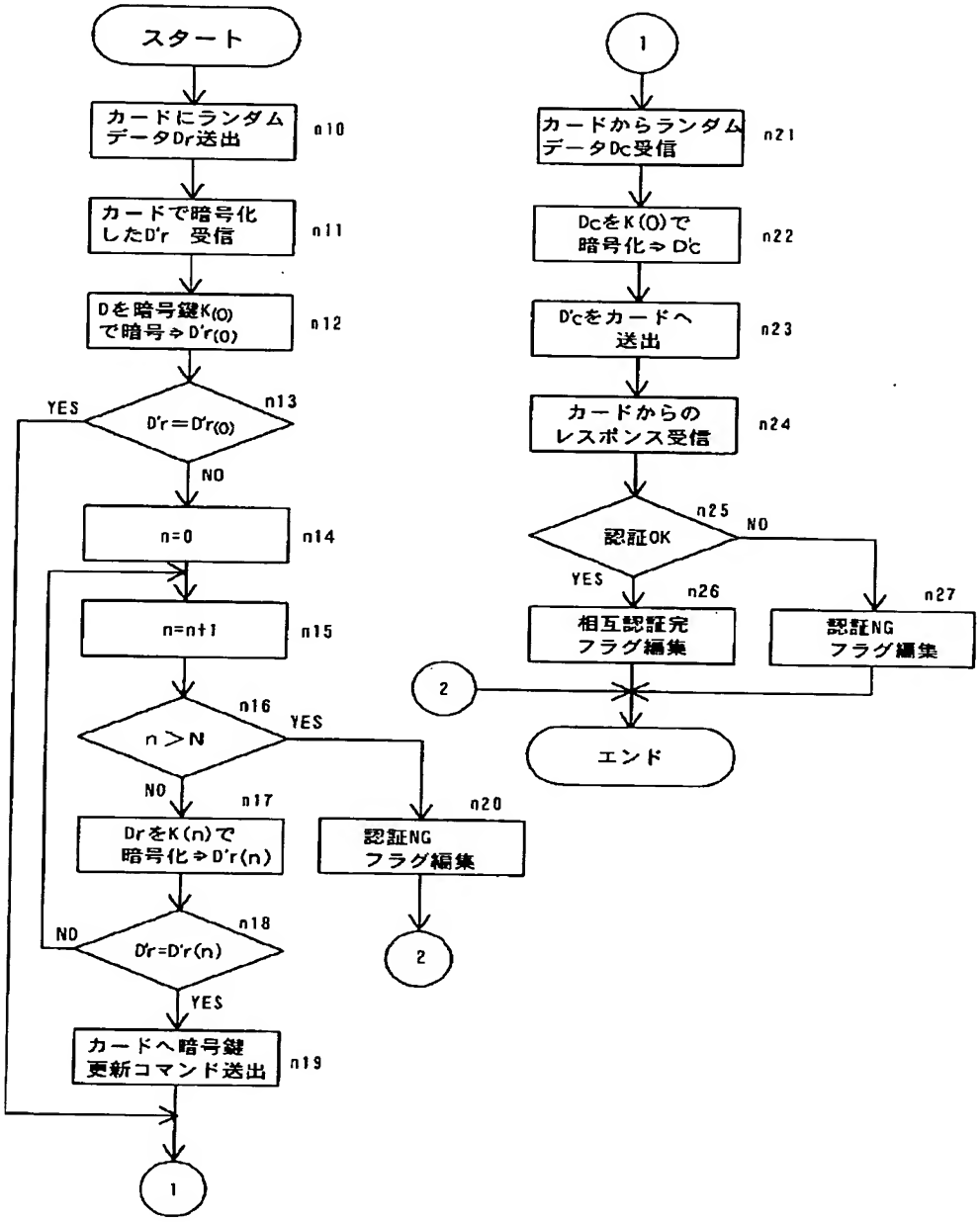
【図５】



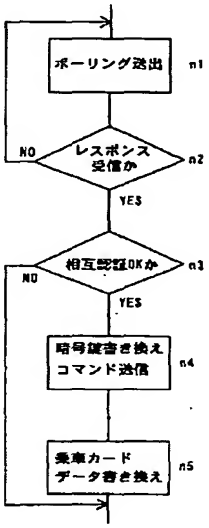
【図６】

暗号鍵	使用期間	状態
暗号鍵１	1998.01.01~1998.03.31	過去に使用
暗号鍵２	1998.04.01~1998.05.10	現在使用中
・・・		未使用
暗号鍵ｎ		未使用

【図９】


スタート
カードにランダムデータDr送出
n10
カードで暗号化したD'r 受信
n11
Dを暗号鍵K(0)で暗号⇒D'r(0)
n12
D'r＝D'r(0)
n13
YES
NO
n=0
n14
n=n+1
n15
n＞N
n16
YES
NO
DrをK(n)で暗号化⇒D'r(n)
n17
D'r=D'r(n)
n18
NO
YES
カードへ暗号鍵更新コマンド送出
n19
1
認証NG フラグ編集
n20
2
1
カードからランダムデータDc受信
n21
DcをK(0)で暗号化⇒D'c
n22
D'cをカードへ送出
n23
カードからのレスポンス受信
n24
認証OK
n25
NO
YES
相互認証完 フラグ編集
n26
認証NG フラグ編集
n27
2
エンド

【図１０】



フロントページの続き

(51)Int.Cl.[7]	識別記号	ＦＩ		ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ	9/00	６７３Ｃ